An Efficient and Secure Identity-based Conditional Privacy-Preserving Scheme in VANETs

Xianglong Wang[1], Qiuting Chen[1], Zhenwan Peng[2], and Yimin Wang[1]
(Corresponding author: Yimin Wang)

The School of Information and Computer, Anhui Agricultural University, Anhui, China[1]
130 Changjiangxilu, Hefei, Anhui, P.R. China
Email: ymw@ahau.edu.cn
The School of Biomedical Engineering, Anhui Medical University, China[2]

(Received Jan. 20, 2022; Revised and Accepted Apr. 28, 2022; First Online May 1, 2022)

Abstract

The existing conditional privacy-preserving identity-based schemes confront the high cost of pseudonym generation and key leakage in Vehicular ad-hoc networks (VANETs). We propose a new anonymous authentication scheme based on identity, aiming to address these issues. In this scheme, the pseudonym of the vehicle is generated by a roadside unit (RSU), reducing the computational pressure of trust authority (TA) or other pseudonym-generating entities. The complete private key of the message signature consists of partial private keys of TA, RSU, and OBU. If adversaries want to generate a legal message signature, they need a complete signature key. As a result, malicious vehicles in VANETs will be easily revoked as long as RSU stops providing pseudonyms and corresponding private keys. The analysis and performance evaluation of the proposed scheme indicate that the scheme has low revocation cost and high message verification and communication efficiency.

Keywords: Vehicular Ad-hoc Networks (VANETs); Conditional Privacy-preserving; Revocation

1 Introduction

With the development of modern science and technology, car ownership increased year by year, but this also caused more road congestion and traffic accident probability. These unpleasant events will affect the driver' s driving state. Therefore, safe and efficient management of road traffic in such cities is an urgent requirement. The rapid development of wireless communication technology (such as GMS, LTE, WiMAX and 5G etc.) provides convenience for intelligent transportation system (ITS), and the traffic generated by thousands of vehicles has been efficiently managed. Vehicular ad-hoc networks (VANETs) play an important role in ITS. VANETs supports two communication modes: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [7]. Through these modes with proper communication technologies, unnecessary accidents could be avoided according to certain information like weather conditions, vehicle location, traffic conditions and road defects [8].

Although having so many benefits, VANETs, like other networks, still meet many problems that are related to authentication and privacy-preserving because of the transparency [1, 14, 17, 22]. Therefore, more and more researchers are paying attention to and studying conditional privacy-preserving authentication schemes. The existing privacy-preserving authentication schemes in VANETs can be classified into three typical authentication schemes: public key infrastructure (PKI) -based, group signature-based and identity-based. ID-based is more efficient and reliable, and it is also one of the most important research directions. So the proposed conditional privacy-preserving authentication scheme is ID-based. ID-based scheme needs to generate a large number of pseudonyms to meet the requirements of anonymity. In some schemes [6,16,23], signatures are generated by trusted authority (TA) or private key generator (PKG), which greatly increase the burden of TA/PKG pseudonyms generation and management. To solve this problem, in He *et al.*'s schemes [11], the pseudonym of the vehicle is generated with the participation of the master key in the TPD. However, side-channel attacks cause sensitive information leakage in tamper-proof device (TPD) [24], and system master key leaks can also make VANETs unsafe. So Wang *et al.* [21] proposed a scheme that does not pre-install the master key in the TPD and generate pseudonyms by the vehicle itself. It effectively prevents the leakage of the master key caused by side-channel attacks, but OBU has limited computing power and may not be able to efficiently generate pseudonyms and message signature. In the scheme proposed by Xiong *et al.* [23], the efficiency of message verification is very high, but the pseudonym is generated in batches by TA, which gives TA great computational pressure. And this scheme does not provide an efficient revocation method. Therefore, this research aims to propose an efficient scheme with conditional privacy-preserving based on Xiong *et al.* [23] and Wang *et al.* [21]. This scheme supports revocation, reducing TA's calculation pressure. The important contributions of this paper include the following:

- We propose a new scheme, which has higher security than existing schemes. Three parts consisted of private key of the signature: the system master key, RSU's private key and OBU's private key. Lacking any part of the key cannot generate a valid signature of message.
- Considering only elliptic curves will be used, our scheme has high verification efficiency and more adaptable to OBU which has limited calculation ability.
- This scheme is able to revoke malicious vehicles efficiently. When a malicious vehicle appears, it can be revoked as long as RSU stops updating its private key.

The composition of the paper is as follows. In Section 2, we introduce briefly the related work on conditional privacy-preserving schemes for VANETs. In Section 3, the background knowledge required for the system model of VANETs based on the proposed scheme is introduced in detail. In Section 4, we describe specifically the proposed scheme. In Section 5, we analyze the security of the proposed scheme. In Section 6, we conduct performance evaluation including validation and communication cost. Finally, we conclude the scheme in Section 7.

2 Related Work

In the introduction, there are existing problems such as communication security, vehicle anonymity and efficiency in VANETs. To improve the security and efficiency of VANETs, researchers have proposed a variety of conditional privacy-preserving authentication schemes for recent years. The existing conditional Privacy-Preserving schemes for VANETs can be divided into three types of authentication schemes: public key infrastructure (PKI) -based, group signature-based and identity-based.

In 2004, Hubaux *et al.* [13] pointed out security and privacy problems in vehicle communication for the first time and proposed a PKI-based scheme. In 2017, Azees M *et al.* [2] proposed a conditional tracking mechanism to trace malicious vehicles or RSUs. In 2021, EF Cahyadi *et al.* [4] proposed an improvement applying a Nonce in the final message. However, the PKI-based scheme requires huge communication overhead due to the storage and management of the certificate lists and the huge computation on the user side.

In 1991, the concept of group signature was proposed by Chaum and van Heyst [5]. In group signature, members of the group are anonymous and can verify the validity of received signature. In 2008, Hao *et al.* [10] proposed a distributed key management scheme which RSU distributes group private keys of a localized way. In 2009, Zhang *et al.* [25] proposed a distributed group authentication scheme, RSU maintains and manages vehicles within their communication range and include vehicles in temporary group. The schemes [10, 25] solve effectively the problems of vehicle privacy protection and the revocation of malicious vehicle in VANETs, but semi-trusted RSU may be attacked. Generally, the group-signature based schemes have the problems of the selection and credibility of group manager and the calculation in group signature.

In 2001, Rives *et al.* [18] proposed the concept of ring signature for the first time. Ring signature is special group signature, in which ring members equally rank and have no administrator. In 2018, Han *et al.* [9] proposed a dual protection scheme for VANETs through RSU auxiliary rings and security data communication. In 2020, Wang *et al.* [20] applied ring selection algorithm to VANETs and select ring members by ring selection algorithm. Obviously, the ring-based signature scheme has a higher level of privacy protection. However, tracking the real identity of malicious vehicles and revoking malicious vehicles are still difficult problems with ring signature-based schemes.

In 1984, Shamir [19] proposed identity-based signature and cryptosystem firstly. In 2013, Lee and Lai [15] proposed an authentication of the batch scheme based on bilinear pairing to enhance the security of VANETs. Horng *et al.* [12] proposed proposed an identity-based verification scheme with higher security and efficiency after correction. In 2015, Lo and Tsai [16] presented a new conditional privacy-preserving authentication scheme based on the elliptic curve cryptosystem to enhance scheme efficiency. In 2019, an efficient certificateless public key signature (CL-PKS) scheme was proposed by Ali *et al.* [1] based on bilinear pairing, they included blockchain to their CL-PKS scheme to improve the security of VANET. In 2022, EF Cahyadi *et al.* [3] summarized recent identity-based batch verification (IBV) schemes and proposed feasible improvements.

In 2020, Wang *et al.* [21] proposed a scheme that does not preinstall the master key of TPD to prevent side channel attacks. However, the limited computing power of OBU cannot efficiently generate pseudonyms and message signature in [21]. Xiong *et al.* [23] claimed that the scheme [15] can not satisfy secure against forgery or the non-repudiation property and guarantee vehicle privacy. Therefore, Xiong *et al.* [23] proposed a cheme aiming at the security flaw in [15]. TA can track the real identity of malicious vehicles. However, the scheme [23] cannot solve the problem of malicious vehicle revocation in VANETs, it does not have revocability. Therefore, we propose

Table 1: Overview table of the advantages of the proposed scheme over existing schemes

	SR-1	SR-2	SR-3	SR-4
Ali *et al.*'s scheme [1]	✗	✓	✗	✓
Horng *et al.*'s scheme [12]	✗	✗	✗	✓
Azees *et al.*'s scheme [2]	✗	✓	✗	✓
Lo *et al.*'s scheme [16]	✓	✗	✓	✗
Wang *et al.*'s scheme [21]	✓	✓	✗	✓
Xiong *et al.*'s scheme [23]	✓	✓	✓	✗
The proposed scheme	✓	✓	✓	✓

[1] SR-1, SR-2, SR-3, SR-4 represent four factors for evaluating the security and efficiency of the scheme, namely no pairing verification, defense against private key stolen attacks, high verification efficiency and revocation, respectively.

[2] ✓:The requirement is satisfied. ✗:The requirement is not satisfied or uninvolved.

an identity-based conditional privacy protection scheme based on Wang *et al.* [21] and Xiong *et al.* [23]. The comparison of some schemes with the proposed scheme are listed in Table 1.

3 Preliminarties

In this section, we describe the system model, security model and mathematical assumptions required to build the proposed scheme.

3.1 System Model

As shown in Figure 1, a complete VANETs consists of trust authority (TA), roadside unit (RSU) fixed on the roadside and on-board unit (OBU) installed on vehicles. The main functions of each entity in VANETs system are described as below.

TA. It is a generally trusted and authoritative entity. TA takes charge of the entire VANETs master key. When VANETs is attacked by malicious vehicles, TA can conduct identity tracking and identity revocation of malicious vehicles through tracking agency (TRA), and remove malicious vehicles from VANETs to ensure the communication security of legitimate vehicles.

RSU. It is a bridge entity that transmits information indirectly. RSU can communicate with OBU through wireless dedicated short-range communication (DSRC) protocol, and can also communicate with TA and application server (AS) through wired network. Therefore, RSU is a bridge between vehicles and TA in VANETs. In our scheme, it is considered malicious but not offensive.

OBU. The vehicle unit OBU is loaded on the vehicle, which contains the tamper-proof device (TPD) module. Information can be transmitted between vehicles and external entities through various external interfaces. Each vehicle broadcasts road traffic information to nearby vehicles every 100–300 ms, such as road congestion and driving state of surrounding vehicles. The communication process is based on DSRC protocol.

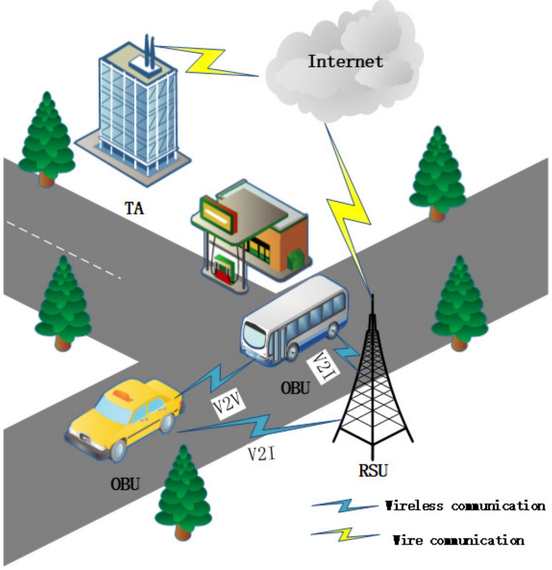

Figure 1: The system model

3.2 Security Model

A secure conditional privacy-preserving authentication scheme should meet the following security requirements.

Message Authentication and Integrity. All vehicle messages in VANETs should ensure that the message is not stolen and tampered by malicious third parties. When receiving the message, the recipient should verify whether the message is sent by the legitimate entity.

Anonymity. Vehicles and other vehicles in VANETs communication, the other vehicle cannot know the real original identity of the vehicle, that is, the receiving vehicle and the sending vehicle are anonymous in communication.

Unlink-ability. Unlink-ability refers that there is no correlation between different information sent by the same user, and the attacker cannot extract sensitive information from different information of the same user.

Traceability. TA can trace the true identity of a vehicle when a malicious vehicle sends malicious messages.

Revocation. If the malicious vehicle is tracked and confirmed, TA can revoke the malicious vehicle from VANETs.

3.3 Mathematic Assumption

First set a finite field $\mathbb{F}_p$, it has prime order p. Then set an elliptic curve defined by equation $y^2 = (x^3 + ax + b) \bmod p$, where $a, b \in \mathbb{Z}_q^*$ and $(4a^3 + 27b^2) \bmod p \neq 0$. An additive elliptic curve group $\mathbb{G}$ of order q is formed by defining $\mathbb{O}$ and some other points on the curve, where q is also a prime and P is the generator of $\mathbb{G}$.

Definition 1. *Elliptic curve discrete logarithm problem (ECDLP): There are two points $(P, W) \in \mathbb{G}$ are given. We consider that no probabilistic polynomial time (PPT) algorithm can calculate the random number $a \in \mathbb{Z}_q^*$ with an unnegligible probability, where a satisfies $W = a \cdot P$.*

Definition 2. *Computational Diffie-Hellman problem (CDHP): On the elliptic curve, some points $\{P, X = a \cdot P, W = b \cdot P\} \in \mathbb{G}$ are given, we consider that no PPT algorithm can calculate $a \cdot b \cdot P \in \mathbb{G}$ with an unnegligible probability, where $a, b \in \mathbb{Z}_q^*$.*

4 The Proposed Scheme

To meet the requirements of conditional privacy-preserve and high-level efficiency authentication in VANETs, we propose a new privacy-preserving scheme. In the proposed scheme, the master key is not preloaded to TPD and the pseudonym generation is executed by RSU. This scheme combines the master key, the private key of the RSU, the virtual ID of the vehicle and generates pseudonyms in the RSU. The scheme consists of six stages: (1) system initialization stage, (2) registration stage, (3) pseudonym and partial key generation stage, (4) key generation stage, (5) message signature stage, (6) message verification stage. Some definitions of notations are shown in Table 2.

4.1 System Initialization Stage

System initialization includes TA initialization and RSU initialization. TA is initialized by generating parameters, it selects randomly $s \in \mathbb{Z}_q^*$ and calculates $P_{pub} = s \cdot P$, in which P_{pub} and s are served as public key and master private key of the system, respectively. Then, TA selects two secure hash functions: $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$; $H_2 : \{0,1\} \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and a homomorphic encryption $Fhomo$. Finally, TA transmits system parameters $\{P, P_{pub}, H_1, H_2, Fhomo\}$ to all RSUs and vehicles. RSU also requires initialization of parameters. The k-th RSU selects a random number $t_{r_k} \in \mathbb{Z}_q^*$ as its private key and calculates $T_{r_k} = t_{r_k} \cdot P$, then broadcasts T_{r_k} as its public key to all vehicles in the area.

Table 2: Notations and description used

Notation	Descriptions
s	The master key of the system
P_{pub}	The pubic key of the system
V_j	The j-th vehicle
RID_j	The real identity of V_j vehicle
VID_j	The vehicle V_j's token issued by TA
$PID_{j,i}$	The i-th pseudonym of the vehicle V_j
t_{r_k}	The k-th RSU's current private key
T_{r_k}	The k-th RSU's current public key
V_{sk_j}	The private key of vehicle V_j
V_{pk_j}	The pubic key of vehicle V_j
H_i	Secure Hash function
$E_{pk}(.)/D_{sk}(.)$	The encryption and the decryption of $Fhomo$
tt_i	Timestamp
$\|$	The message concatenation operation
$\oplus$	The exclusive-OR operation

4.2 Registration Stage

Vehicles must register offline to TA before they join VANETs. Vehicle V_j submits real identity RID_j to TA for validation(this identity must be legal in real life such as owner's identity card or license plate, as it is a necessary condition for tracking entity identity). If RID_j is valid, TA selects randomly a number $\alpha_{j,i} \in \mathbb{Z}_q^*$ as part of the vehicle's message signature key, it calculates $VID_j = RID_j \oplus \alpha_{j,i} \cdot P_{pub}$ as a virtual ID of the vehicle V_j in VANETs. Then TA selects randomly a number $V_{sk_j} \in \mathbb{Z}_q^*$, and compute $V_{pk_j} = V_{sk_j} \cdot P$ where V_{sk_j} is the private key of V_j and V_{pk_j} is the public key of V_j. Finally, parameter $pv_j = \{VID_j, SIG_s(VID_j), V_{pk_j}, V_{sk_j}\}$ is preloaded into TPD to generate pseudonyms and partial keys. TPD does not storage sensitive parameters in this step. The process of the registration stage is shown in Algorithm 1.

Algorithm 1 Vehicle Registration (Executed by TA)

```
Input: the system master key $s$, the vehicle $V_j$ real identity $RID_j$.
Output:
Selects a random number $\alpha_{j,i}, V_{sk_j} \in \mathbb{Z}_q^*$
Computes $VID_j = RID_j \oplus \alpha_{j,i} \cdot P_{pub}$
Computes the signature $SIG_s(VID_j)$
Computes $V_{pk_j} = V_{sk_j} \cdot P$
return $pv_j = \{VID_j,\ SIG_s(VID_j),\ V_{pk_j},\ V_{sk_j}\}$
```

4.3 Pseudonym and Partial Key Generation Stage

When the vehicle V_j enters a new RSU area, the OBU will submits $\{VID_j,\ SIG_s(VID_j),\ V_{pk_j}\}$ to the RSU. When RSU receives the message, it will retransmit the message to TA for verifying the legitimacy of the vehicle. If the vehicle is legal, TA will return the tuple $\{\epsilon_{j,i},\ Q_j\}$ to RSU, where $\epsilon_{j,i} = E_{T_{r_k}}(s + \alpha_{j,i})$ and $Q_j = \alpha_{j,i} \cdot P$. Finally, the RSU calculates and returns the tuple $\{A_{j,i}, PID_{j,i}, E_{V_{pk_j}}(\delta_{j,i})\}$ $(i = 1, ..., n\ )$ to the vehicle, where $\delta_{j,i}$ is a partial signature key. Process as shown in Algorithm 2 to calculate parameters.

Algorithm 2 Generation of Pseudonym and Private Key (Executed by RSU)

```
Input: the ciphertext $\{\epsilon_{j,i}, Q_j\ \}$ $(i = 1, ..., n)$.
Output:
Selects a random number $k_{j,i} \in \mathbb{Z}_q^*$
Then computes
    $\begin{cases} B_{j,i} = D_{t_{r_k}}(\epsilon_{j,i}) + t_{r_k} = s + \alpha_{j,i} + t_{r_k} \\ PID_{j,i} = VID_j \oplus H(k_{j,i} \parallel P_{pub} \parallel Q_j) \\ h_{j,i} = H_1(PID_{j,i} \parallel P_{pub} \parallel T_{r_k} \parallel Q_j) \\ A_{j,i} = k_{j,i} \cdot P + h_{j,i} \cdot Q_j \\ \delta_{j,i} = k_{j,i} + h_{j,i} \cdot B_{j,i} \end{cases}$
return $\{A_{j,i}, PID_{j,i}, E_{V_{pk_j}}(\delta_{j,i})\ \}$ $(\ i = 1, ..., n\ )$
```

4.4 Key Generation Stage

If a vehicle needs to communicate with another vehicle or RSU, OBU needs to sign a message and attach a timestamp to generate a message tuple.

The tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ are calculated when the vehicle receives the tuple $\{A_{j,i}, PID_{j,i}, E_{V_{pk_j}}(\delta_{j,i})\ \}$ returned by the RSU, as illustrated in Algorithm 3.

Finally, the OBU broadcasts message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ to RSU and all vehicles in the area, and $\gamma_{j,i}$ is the signature of the message.

Algorithm 3 Signature Generation (Executed by OBU)

```
Input: the ciphertext $\{A_{j,i}, PID_{j,i}, E_{V_{pk_j}}(\delta_{j,i})\}$.
Output:
Computes $h_{j,i} = H_1(PID_{j,i} \parallel P_{pub} \parallel T_{r_k} \parallel Q_j)$
Computes $h'_{j,i} = H_2(PID_{j,i} \parallel M \parallel T_{r_k} \parallel tt_i)$
Computes $\delta_{j,i} = D_{V_{sk_j}}(\delta_{j,i}) = k_{j,i} + h_{j,i} \cdot B_{j,i}$
Computes $\gamma_{j,i} = \delta_{j,i} + h'_{j,i} \cdot V_{sk_j}$
return $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$
```

4.5 Message Verification Stage

4.5.1 Single Verification

The message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ can be verified by the RSU or all vehicles in the area. At first, the recipient will check whether the timestamp tt_i is refreshed, if not, the message will be rejected, else the following equation will continue to be verified:

$$\gamma_{j,i} \cdot P == A_{j,i} + h_{j,i} \cdot (P_{pub} + T_{r_k}) + h'_{j,i} \cdot V_{pk_j} \qquad (1)$$

The recipient will trusts the message if Equation (1) is satisfied, or rejects the message if not.

If the message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ is not tampered in the transmission process, it will satisfy the equation(1). Since $\gamma_{j,i} = \delta_{j,i} + h'_{j,i} \cdot V_{sk_j}$, $\delta_{j,i} = k_{j,i} + h_{j,i} \cdot B_{j,i}$ and $B_{j,i} = s + \alpha_{j,i} + t_{r_k}$, where $h_{j,i} = H_1(PID_{j,i} \parallel P_{pub} \parallel T_{r_k} \parallel Q_j)$, and $h'_{j,i} = H_2(PID_{j,i} \parallel M \parallel T_{r_k} \parallel tt_i)$, so we have the following:

$$\begin{aligned} \gamma_{j,i} \cdot P &= (k_{j,i} + h_{j,i} \cdot B_{j,i} + h'_{j,i} \cdot V_{sk_j}) \cdot P \\ &= k_{j,i} \cdot P + h_{j,i} \cdot (s + \alpha_{j,i} + t_{r_k}) \cdot P + h'_{j,i} \cdot V_{sk_j} \cdot P \\ &= A_{j,i} + h_{j,i} \cdot (P_{pub} + T_{r_k}) + h'_{j,i} \cdot V_{pk_j} \end{aligned}$$

Therefore, the scheme can correctly validate single messages. The process of message verification such as Algorithm 4.

4.5.2 Batch Verification

This scheme also supports batch verification of multiple messages received. When the recipient receives multiple messages, the recipient can verify whether Equation (2) satisfies.

$$\begin{aligned} \left(\sum_{j,i=0}^{n} (d_{j,i} \cdot \gamma_{j,i})\right) \cdot P = \sum_{j,i=0}^{n} d_{j,i} \cdot A_{j,i} \\ + \left(\sum_{j,i=0}^{n} (d_{j,i} \cdot h_{j,i})\right) \cdot (P_{pub} + T_{r_k}) \\ + \sum_{j,i=0}^{n} \left((d_{j,i} \cdot h'_{j,i}) \cdot V_{pk_j}\right) \end{aligned} \qquad (2)$$

In the equation, $d_{1,i}, d_{2,i}, ..., d_{n,i} \in [1, 2^t]$, where t is a small integer.

Algorithm 4 Message Verification (Executed by Vehicle or RSU)

```
Input: the message tuple$\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$.
Output:
Checks whether the timestamp $tt_i$ is refreshed, if not, rejects
if $tt_i$ is fresh then
    Computes $h_{j,i} = H_1(PID_{j,i} \parallel P_{pub} \parallel T_{r_k} \parallel Q_j)$
    Computes $h'_{j,i} = H_2(PID_{j,i} \parallel M \parallel T_{r_k} \parallel tt_i)$
    if $\gamma_{j,i} \cdot P == A_{j,i} + h_{j,i} \cdot (P_{pub} + T_{r_k}) + h'_{j,i} \cdot V_{pk_j}$ then
        return true
    else
        return false
    end if
else
    return false
end if
```

The proof process is as follows :

$$\left(\sum_{j,i=0}^{n}(d_{j,i} \cdot \gamma_{j,i})\right) \cdot P$$

$$= \sum_{j,i=0}^{n} d_{j,i} \cdot (k_{j,i} + h_{j,i} \cdot B_{j,i} + h'_{j,i} \cdot V_{sk_j}) \cdot P$$

$$= \sum_{j,i=0}^{n} d_{j,i} \cdot A_{j,i} + \left(\sum_{j,i=0}^{n}(d_{j,i} \cdot h_{j,i})\right) \cdot (P_{pub} + T_{r_k})$$

$$+ \sum_{j,i=0}^{n}\left((d_{j,i} \cdot h'_{j,i}) \cdot V_{pk_j}\right)$$

Therefore, the scheme can validate multiple messages correctly.

5 Scheme Analysis

In this section, we will analyze the security and privacy of our scheme.

5.1 Message Integrity

This scheme divides the key generation of message signature into three parts: the system master key, RSU's private key and OBU's private key. When missing any part of the key, the message signature cannot be generated. In addition, as long as ECDLP is difficult to be solved, the attacker cannot forge a vaild message signature. Therefore, if the signature and the message tuple satisfy the equation $\gamma_{j,i} \cdot P == A_{j,i} + h_{j,i} \cdot (P_{pub} + T_{r_k}) + h'_{j,i} \cdot V_{pk_j}$, authentication and integrity of the message can be guaranteed according to the above verification process.

5.2 Anonymity and Unlink-ability

In the process of generating pseudonyms, $PID_{j,i} = VID_j \oplus H(k_{j,i} \parallel P_{pub} \parallel Q_j)$, where $k_{j,i}$ is a number selected randomly by RSU without any valuable information, so the scheme can meet the requirements of anonymity. Each vehicle's message is sent under a different pseudonym. These pseudonyms that are randomly generated on RSU with no correlation, so the scheme can meet the requirements of Unlink-ability.

5.3 Traceability

The message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ that sent by the vehicle includes the pseudonym $PID_{j,i}$, where $PID_{j,i} = VID_j \oplus H(k_{j,i} \parallel P_{pub} \parallel Q_j)$, so TA can calculate

$$VID_j = PID_{j,i} \oplus H(k_{j,i} \parallel P_{pub} \parallel Q_j)$$
$$RID_j = VID_j \oplus \alpha_{j,i} \cdot P_{pub}$$

to get the real identity RID_j of the vehicle.

5.4 Revocation

When the real identity of the malicious vehicle is confirmed, it will be added to the revocation list, and TA will notify the RSU in the area where the malicious vehicle is located. RSU will update its private key t'_{r_k} and public key T'_{r_k} after receiving revocation instructions that sent by TA. RSU retransmits partial message signature key tuple $\{ A'_{j,i}, PID'_{j,i}, E_{V_{pk_j}}(\delta'_{j,i})\}(i = 1, ..., n)$ to normal legitimate vehicles. However, the parameters of malicious vehicles are not updated, so the above proof process is not satisfied, namely $\gamma_{j,i} \cdot P \neq A_{j,i} + h_{j,i} \cdot (Pub + T'_{r_k}) + h'_{j,i} \cdot V_{pk_j}$, since T_{r_k} is obviously not equal to T'_{r_k}. Therefore, RSU and other vehicles no longer trust messages taht sent by malicious vehicles. So the scheme supports the revocation of malicious vehicles.

5.5 Resist Multiple Types of Attacks

In this subsection, we will demonstrate and analyze the ability of the scheme to resist five common attacks.

Simulating Attacks. Assume that an attacker can forge and generate a valid message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$. This means that the attacker can forge the valid signature of vehicle V_j. We have already analyzed the reliability and integrity of the message of the scheme, that is, the attacker cannot forge a valid signature, because the forgery is impossible unless three partial keys are obtained at the same time. The probability of forging legitimate message signatures can be ignored.

Tampering Attacks. Suppose an attacker can forge and generate message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ of vehicle V_j. It means that the attacker can forge the valid signature

Table 3: Operations and description used

Operations	Descriptions	Time(ms)
t_{bp}	The execution time of a bilinear pairing operation	4.211
t_{bpm}	The execution time of a scalar multiplication operation related to the bilinear pairing	1.709
t_{bpa}	The execution time of a point addition operation related to the bilinear pairing	0.0071
t_{em}	The execution time of a scalar multiplication operation	0.442
t_{esm}	The execution time of a small scale multiplication operation	0.0138
t_{mtp}	The time to perform a MapToPoint operation	4.406

of vehicle V_j, but the operation process of message signature ensures the uniqueness of the message. This is almost impossible without solving the ECDLP.

Repeat Attacks. When the recipient receives the message, at first it will check whether the timestamp tt_i is refreshed. Repeated message tuple will be rejected by the recipient. Therefore, the scheme can resist repeated attacks.

Man-in-the-middle Attacks. In the above analysis, all messages must be signed, and the message signatures cannot be forged without obtaining the private key. Therefore, the proposed scheme can resist man-in-the-middle attack.

Private Key Stolen Attacks. In the scheme, the signature of the message requires completed system private key s, RSU's private key t_{r_k} and OBU's private key V_{sk_j}. Even if the system master key s or the vehicle private key V_{sk_j} are leaked to the adversary under a side-channel attack, it is still unable to generate a valid message signature. Therefore, the scheme can resist private key stolen attacks.

6 Performance Evaluation

In this section, we will evaluate the performance of the scheme, which includes verification and communication costs. In addition, we will compare the scheme with other existing schemes in VANETs. We set the security level to 80 bits and use an elliptic curve additive group $\mathbb{G}$, which means p and q are primes of two 160 bits. Here we use a bilinear pairing: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ to ensure that the security level is 80 bits, where $\mathbb{G}_1$ is the additive group on the elliptic curve, and the embedding degree is 2. We ignore the time required for general hash operation, XOR operation and general multiplication. In the scheme, the vehicle pseudonym is generated by RSU that has super computing power. Therefore, we do not consider to compare the time of signature generation in comparison. We adopt the experiment and evaluation method in [25]. According to the experiment in [25], we show that the execution time and description of the main encryption operations are listed in Table 3.

6.1 Verification Cost

The cryptographic operations in the schemes of Ali *et al.* [1], Azees *et al.* [2] and Horng *et al.* [12] are based on bilinear pairing, the scalar multiplications are performed on elliptic curves that is related to bilinear pairing. The cryptographic operations in the schemes of Wang *et al.* [21], Lo *et al.* [16], Xiong *et al.* [23] and the proposed scheme, the scalar multiplication is performed on a given elliptic curve. We will analyze the execution time of one message single verification and multiple message batch verification in detail for the above four schemes.

For the single verification of Ali *et al.* [1], the vehicle needs to execute one bilinear pairing operation, one scalar multiplication operation and one point addition operation that are related to bilinear pairing, therefore, the time that required to verify the single message is $1t_{bp}+1t_{bpm}+1t_{bpa} \approx 5.9271$ ms; for the batch verification of multiple messages, the verifier needs to execute one bilinear pairing operation, n scalar multiplication operations and n point additions operations that are related to bilinear pairing, therefore, the time that required to verify n messages is $t_{bp}+nt_{bpm}+nt_{bpa} \approx 1.7161n+4.211$ ms. Similarly, in the scheme of Horng *et al.* [12], the time that required to verify the single message is $2t_{bp}+2t_{bpm}+1t_{mtp} \approx 16.246$ ms, the time that required to verify n messages is $2t_{bp}+2nt_{bpm}+nt_{mtp} \approx 7.824n+8.422$ ms. In the scheme of Azees *et al.* [2], the time that required to verify the single message is $2t_{bp}+5t_{bpm}+2t_{bpa} \approx 16.9812$ ms, the time that required to verify n messages is $(n+1)t_{bp}+5nt_{bpm}+2nt_{bpa} \approx 12.7702n+4.211$ ms.

For the single verification of proposed scheme, the vehicle needs to execute three scalar multiplication operations and one small scale multiplication operation, therefore, the time that required to verify the single message is $3t_{em}+1t_{esm} \approx 1.3398$ms; for the batch verification of multiple messages, the verifier needs to execute $(n+2)$ scalar multiplication operations and n small scale multiplication operations, therefore, the time that required to verify n messages is $(n+2)t_{em}+nt_{esm} \approx 0.4558n+0.884$ ms. Similarly, in the scheme of Wang *et al.* [21], the time that required to verify the single message is $4t_{em} \approx$

Table 4: Comparison of verification cost

Schemes	Single verification(ms)	Batch verification (ms)
Ali *et al.*'s scheme [1]	$1t_{bp} + 1t_{bpm} + 1t_{bpa} \approx 5.9271$	$t_{bp} + nt_{bpm} + nt_{bpa} \approx 1.7161n + 4.211$
Horng *et al.*'s scheme [12]	$2t_{bp} + 2t_{bpm} + 1t_{mtp} \approx 16.246$	$2t_{bp} + 2nt_{bpm} + nt_{mtp} \approx 7.824n + 8.422$
Azees *et al.*'s scheme [2]	$2t_{bp} + 5t_{bpm} + 2t_{bpa} \approx 16.9812$	$(n+1)t_{bp} + 5nt_{bpm} + 2nt_{bpa} \approx 12.7702n + 4.211$
Lo *et al.*'s scheme [16]	$3t_{em} \approx 1.326$	$(n+2)t_{em} + 2nt_{esm} \approx 0.4696n + 0.884$
Wang *et al.*'s scheme [21]	$4t_{em} \approx 1.768$	$(2n+3)t_{em} + 2nt_{esm} \approx 0.9116n + 1.326$
Xiong *et al.*'s scheme [23]	$3t_{em} + t_{esm} \approx 1.3398$	$(n+2)t_{em} + nt_{esm} \approx 0.4558n + 0.884$
The proposed scheme	$3t_{em} + t_{esm} \approx 1.3398$	$(n+2)t_{em} + nt_{esm} \approx 0.4558n + 0.884$

1.768 ms, the time that required to verify n messages is $(2n+3)t_{em} + 2nt_{esm} \approx 0.9116n + 1.326$ ms. In the scheme of Lo *et al.* [16], the time that required to verify the single message is $3t_{em} \approx 1.326$ ms, the time that required to verify n messages is $(n+2)t_{em} + 2nt_{esm} \approx 0.4696n + 0.884$ ms. In the scheme of Xiong *et al.* [23], the time that required to verify the single message is $3t_{em} + t_{esm} \approx 1.3398$ ms, the time that required to verify n messages is $(n+2)t_{em} + nt_{esm} \approx 0.4558n + 0.884$ ms.

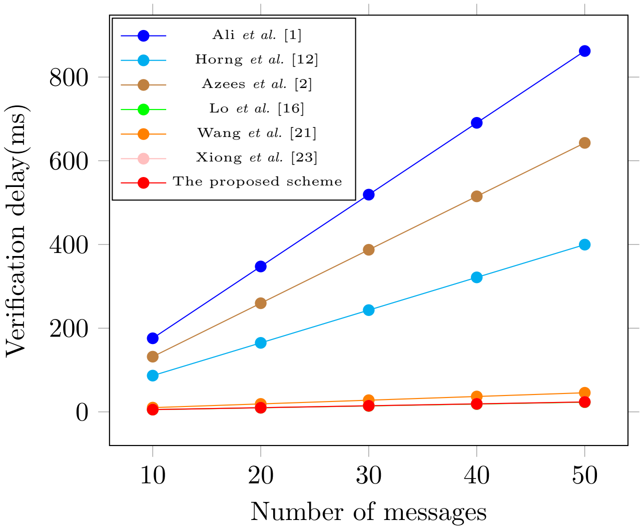

Figure 2: Verification operation cost of multiple messages

The calculation cost comparison of all schemes is listed in Table 4. Figure 2 shows a comparison of the verification cost of the scheme. According to Table 4 and Figure 2, the proposed scheme, the schemes of Lo *et al.* [16], Wang *et al.* [21] and Xiong *et al.* [23] have higher certification efficiency than the schemes of Horng *et al.* [12], Azees *et al.* [2] and Ali *et al.* [1], since these schemes use elliptic curve encryption instead of bilinear pairing. Compared with other schemes, the proposed scheme does not preload the master key of the system into TPD, and generate pseudonyms by RSU. Therefore, the proposed scheme has higher security and pseudonym generation efficiency.

6.2 Communications Cost

In this subsection, we will analyze the other communication costs of the proposed scheme, which includes the communication costs in addition to the message itself, such as signature, pseudonym, certificate and so on. Communication costs for five schemes are listed in Table 5.

Table 5: Comparison of communication cost

Schemes	a message(bytes)	n message (bytes)
Ali *et al.* [1]	536	536n
Horng *et al.* [12]	388	388n
Azees *et al.* [2]	848	848n
Lo *et al.* [16]	188	188n
Wang *et al.* [21]	124	124n
Xiong *et al.* [23]	128	128n
The proposed scheme	124	124n

In the scheme of Ali *et al.* [1], the vehicle broadcasts $\{AID_{i,1}, AID_{i,2}, X_i, Y_i, \theta, t_i\}$ to the recipient, where $AID_{i,1}, X_i, Y_i, \theta \in \mathbb{G}_1, AID_{i,2} \in \mathbb{Z}_q^*$ and t_i is the time stamp. Therefore, the communication cost is $4*128+20+4 = 536$ bytes. In Horng *et al.*'s scheme [12], the vehicle broadcasts $\{PID_i^1, PID_i^2, \sigma\}$ to the recipient, where $PID_i^1, PID_i^2, \sigma \in \mathbb{G}_1$, thus the communication cost is $3*128+4 = 388$ bytes. In Azees *et al.*'s scheme [2], the vehicle broadcasts its signature messages $\{sig \parallel Y_k \parallel Cert_k\}$ to the verifier, where $Cert_k = \{Y_k \parallel E_i \parallel DID_{ui} \parallel \gamma_u \parallel \gamma_v \parallel c \parallel \lambda \parallel \sigma_1 \parallel \sigma_2\}$, $\{sig, E_i, DID_{ui}, \gamma_u, \gamma_v, Y_k\} \in \mathbb{G}_1, \{\lambda, \sigma_1, \sigma_2\} \in \mathbb{Z}_q^*$, thus the communication cost is $6*128+4*20 = 848$ bytes. In Lo *et al.*'s scheme [16], the vehicle broadcasts $\{PID_i = (PID_{i,1}, PID_{i,2}, t_i), tt_i, \delta = (K_i, R_i, V_i)\}$ to the recipient, where $PID_{i,1}, K_i, R_i, V_i \in \mathbb{G}$, $PID_{i,2} \in \mathbb{Z}_q^*$ and t_i, tt_i are timestamps, thus the communication cost is $4*40+20+4*2 = 188$ bytes. In Wang *et al.*'s scheme [21], the vehicle broadcasts $\{PID_{i,j} = (PID1_{i,j}, PID2_{i,j}), U_{i,j}, V_{i,j}, tt_i\}$ to the recipient, where $PID2_{i,j}, U_{i,j} \in \mathbb{G}$, $PID1_{i,2}, V_{i,j} \in \mathbb{Z}_q^*$ and tt_i is timestamp, thus the communication cost is $2*40+2*20+4 = 124$ bytes. In Xiong *et al.*'s scheme [23], the vehicle broadcasts $\{A_{j,i}, PID_{j,i}, S_{pub_j}, T_{j,i}, \beta_{j,i}, t_{j,i}\}$ to the recipient, where $A_{j,i}, S_{pub_j} \in \mathbb{G}$, $PID_{j,i}, \beta_{j,i} \in \mathbb{Z}_q^*$ and $T_{j,i}$, tt_i are timestamps, thus the communication cost is $2*40+2*20+4*2 = 128$ bytes. In the proposed scheme, the vehicle broadcasts message tuple $\{A_{j,i}, M, PID_{j,i}, V_{pk_j}, \gamma_{j,i}, tt_i\}$ to the surrounding receiving unit, where $A_{j,i}, V_{pk_j} \in \mathbb{G}$, $PID_{j,i}, \gamma_{j,i} \in \mathbb{Z}_q^*$ and tt_i is time stamp. Therefore the communication cost is $2*40+2*20+4 = 124$ bytes. The communication costs of the five schemes are shown in Figure 3. According to the Figure 3, the proposed scheme has a very low communication cost compared with other schemes.

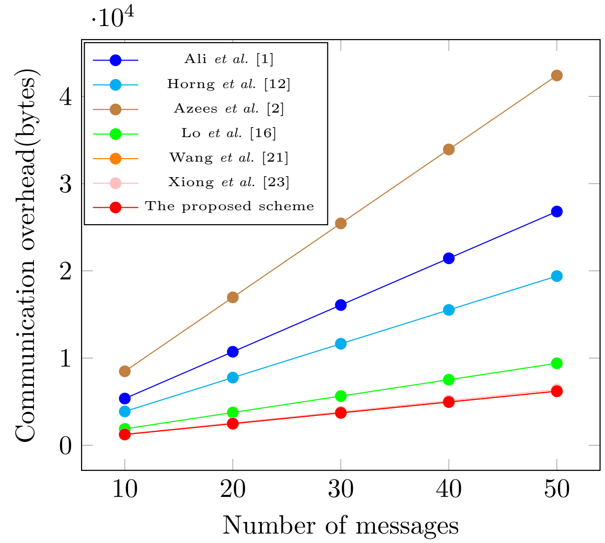

Figure 3: Communication cost of multiple messages

7 Conclusion

In this study, a secure and efficient conditional privacy-preservation scheme that based on identity for V2V and V2I communication in VANETs has been proposed. Since the signature key of the vehicle message is generated by the private key of TA, RSU and vehicle itself, the message will not be signed if any part of the private key is missing, so this scheme can stop attacker forging the message. In addition, the pseudonym is generated by RSU, which reduces the burden of TA calculation and pseudonym management. It also means that malicious vehicles can be effectively revoked from VANETs as long as the RSU stops providing pseudonyms and corresponding private keys. Performance evaluation results reveal that the scheme has higher verification efficiency and lower communication cost.

Acknowledgments

This research was supported by Anhui Provincial Natural Science Foundation (2108085QF274) and Talent Foundation of agricultural university (rc482005).

References

[1] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in vanets," *Journal of Systems Architecture*, vol. 99, p. 101636, 2019.

[2] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[3] E. F. Cahyadi, C. Damarjati, and M. S. Hwang, "Research on identity-based batch verification schemes for security and privacy in vanets," *Journal of Electronic Science and Technology*, vol. 20, no. 3, pp. 1–19, 2022.

[4] E. F. Cahyadi and M. S. Hwang, "An improved efficient anonymous authentication with conditional privacy-preserving scheme for vanets," *Plos one*, vol. 16, no. 9, p. e0257044, 2021.

[5] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1991, pp. 257–265.

[6] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654–1667, 2019.

[7] M. Gonzalez-Martín, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of c-v2x mode 4 vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1155–1166, 2018.

[8] M. M. Hamdi, L. Audah, S. A. Rashid, and M. Al Shareeda, "Techniques of early incident detection and traffic monitoring centre in vanets: A review." *Journal of Communications*, vol. 15, no. 12, pp. 896–904, 2020.

[9] Y. Han, N. N. Xue, B. Y. Wang, Q. Zhang, C. L. Liu, and W. S. Zhang, "Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 20 209–20 220, 2018.

[10] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against rsu compromise in group signature based vanets," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, pp. 1–5, 2008.

[11] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[12] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[13] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[14] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383–393, 2015.

[15] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for vanet," *Wireless networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[16] N. W. Lo and J. L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2015.

[17] B. Palaniswamy, S. Camtepe, E. Foo, and J. Pieprzyk, "An efficient authentication scheme for intra-vehicular controller area network," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3107–3122, 2020.

[18] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, pp. 552–565, 2001.

[19] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*. Springer, pp. 47–53, 1984.

[20] L. Wang, X. Lin, L. Qu, and C. Ma, "Ring selection for ring signature-based privacy protection in vanets," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–6, 2020.

[21] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, 2020.

[22] L. Wu, Y. Xia, Z. Wang, and H. Wang, "Be stable and fair: Robust data scheduling for vehicular networks," *IEEE Access*, vol. 6, pp. 32 839–32 849, 2018.

[23] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, "CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in vanets," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3456–3468, 2021.

[24] T. Zaidi and S. Faisal, "An overview: Various attacks in vanet," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*. IEEE, pp. 1–6, 2018.

[25] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2009.

Biography

Xianglong Wang is a student at the School of Information and Computer Science, Anhui Agricultural University. His research interest is privacy security protection in wireless communication.

Qiuting Chen is a student at the School of Information and Computer Science, Anhui Agricultural University. Her research interests is network information security.

Zhenwan Peng is now a Lecturer in the School of Biomedical Engineering, Anhui Medical University. He received the Ph.D. degree from Anhui University of China, in 2018. His research interest includes classical and quantum cryptography, in particular, secure multiparty computations.

Yimin Wang is now an Associate Professor in the School of Computer Science and Technology, Anhui Agriculture University. He received PhD degree in Anhui University of China. His research interests include security and privacy for wireless networks, cloud computing, big data, etc..